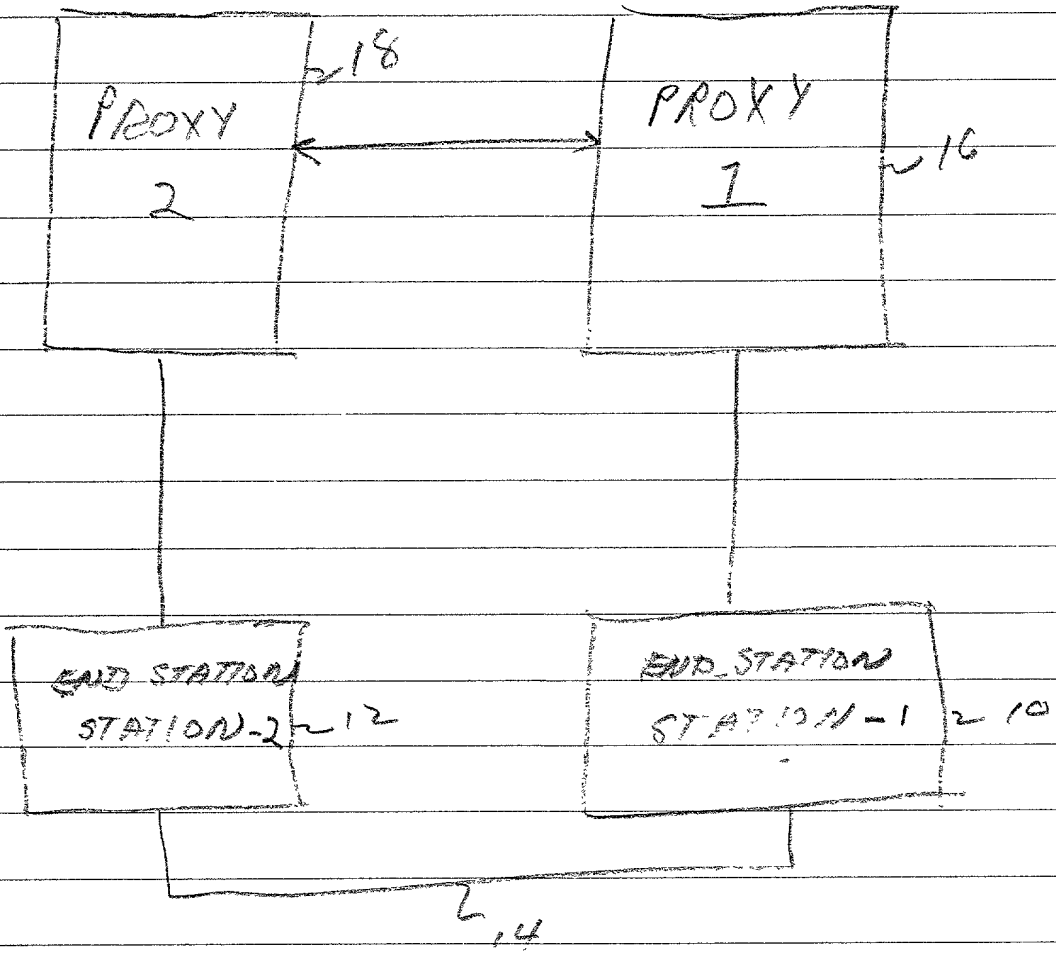
PROXY
2
18
PROXY
1
16
END STATION
STATION-2
12
END STATION
STATION-1
10
14

FIG 1

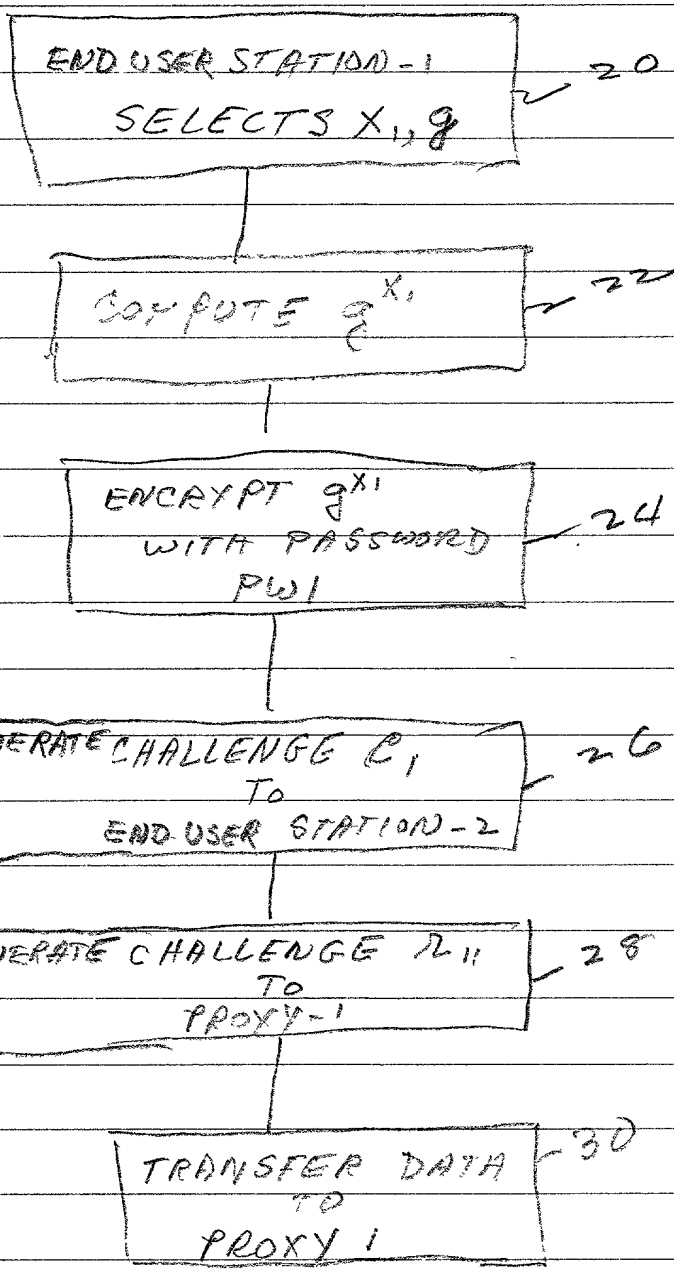
END USER STATION-1
SELECTS X_1, g
20
COMPUTE g^{X_1}
22
ENCRYPT g^{X_1}
WITH PASSWORD
PW1
24
GENERATE CHALLENGE C_1
TO
END USER STATION-2
26
GENERATE CHALLENGE R_{11}
TO
PROXY-1
28
TRANSFER DATA
TO
PROXY 1
30

FIG 2

PROXY-1 RECEIVES $PW_1(g^{x_1})$ C_1, r_{11} — 32

DECRYPTS $PW_1(g^{x_1})$ — 34

STORE g^{x_1} r_{11} — 36

PICK SECRET # y_1
COMPUTE $g^{x_1 y_1}$ — 38

CONCATENATE $g^{x_1 y_1} || C_1$ — 39

DIGITALLY SIGN $g^{x_1 y_1} || C_1$ — 40

RETRIEVE PROXY-1 CERTIFICATE-1 — 42

TRANSMITS SIGNED($g^{x_1 y_1} || C$), CERT 1 TO PROXY 2 — 44

FIG 3

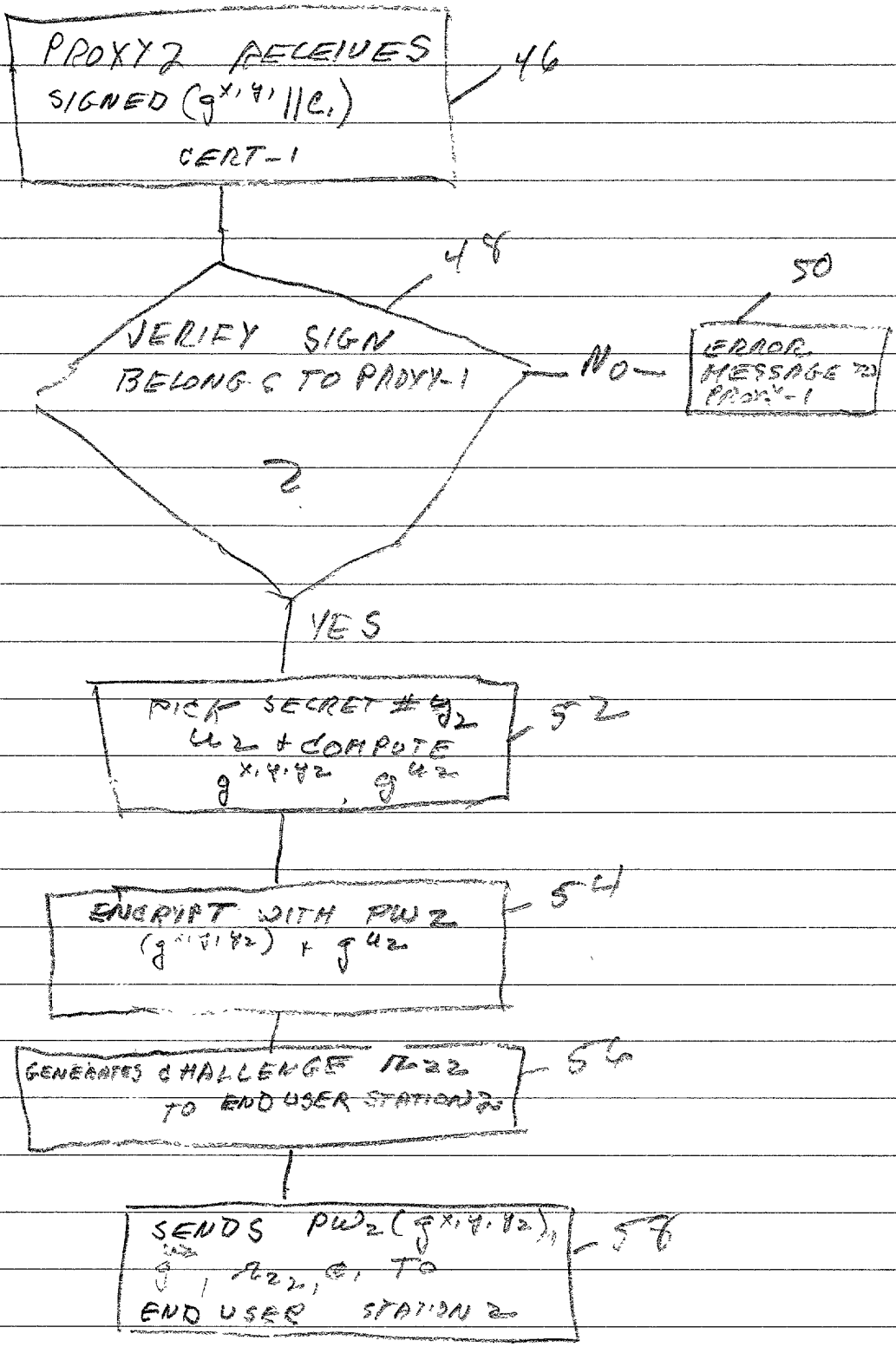
PROXY 2 RECEIVES
SIGNED ($g^{x,y}$ || C_1)
CERT-1
46
48
VERIFY SIGN
BELONG C TO PROXY-1
NO
50
ERROR MESSAGE TO PROXY-1
2
YES
PICK SECRET # y_2
u_2 + COMPUTE
g^{x,y,y_2}, g^{u_2}
52
ENCRYPT WITH PW_2
(g^{x,y,y_2}) + g^{u_2}
54
GENERATES CHALLENGE R_{22}
TO END USER STATION 2
56
SENDS $PW_2(g^{x,y,y_2})$,
g^{y_2}, R_{22}, C_1 TO
END USER STATION 2
58

FIG 4

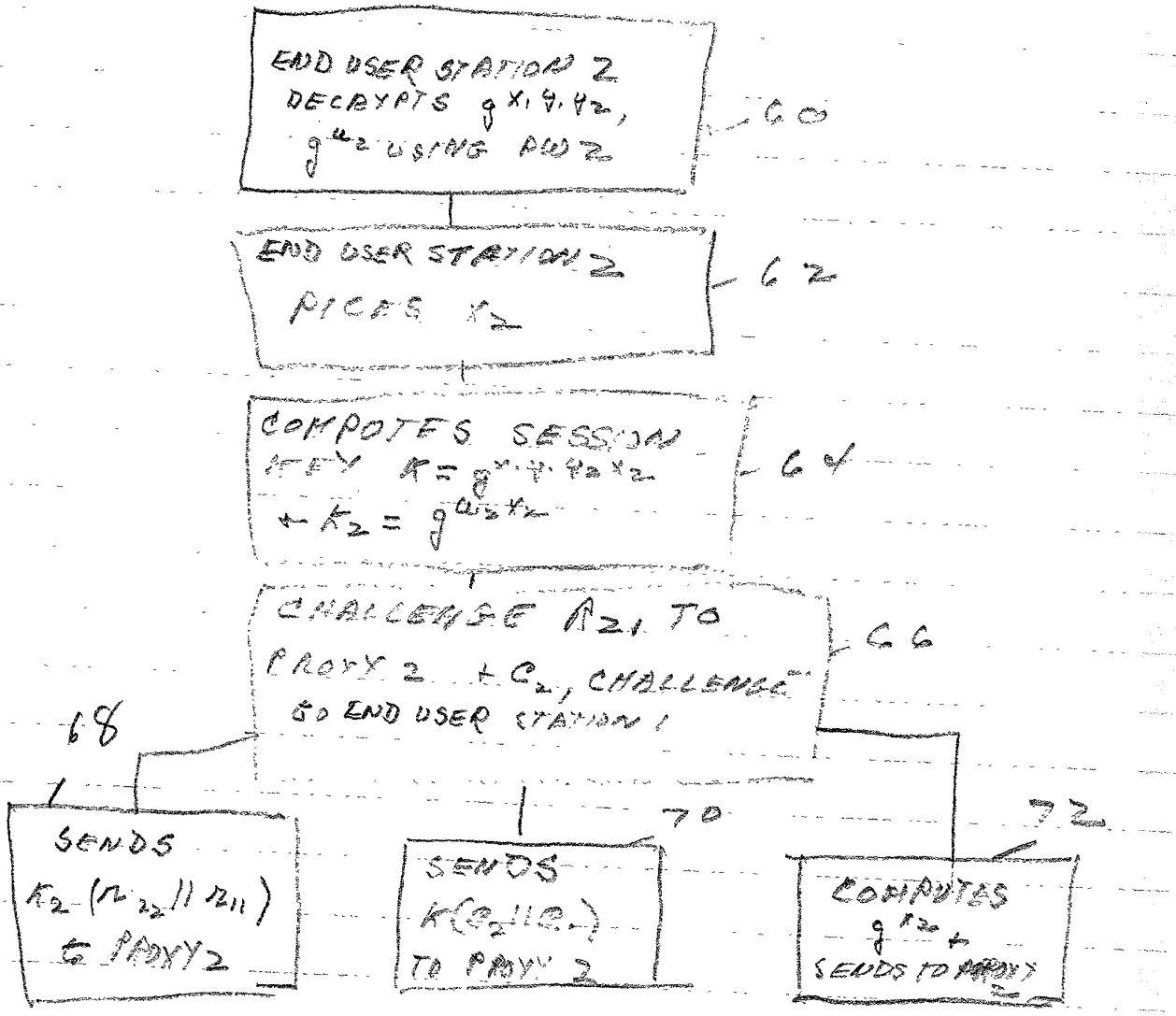
END USER STATION 2 DECRYPTS g^{x_1}, Φ, Φ_2, g^{ω_2} USING PW 2
60
END USER STATION 2 PICKS x_2
62
COMPUTES SESSION KEY $K = g^{x_1 \cdot x_2 \cdot \Phi_2 \cdot x_2}$ & $K_2 = g^{\omega_2 x_2}$
64
CHALLENGE Φ_{21} TO PROXY 2 & C_2, CHALLENGE TO END USER STATION 1
66
68
SENDS $K_2(\Phi_{22} \| \Phi_{11})$ TO PROXY 2
70
SENDS $K(C_2 \| C_1)$ TO PROXY 2
72
COMPUTES g^{Φ_2} & SENDS TO PROXY

FIG 5

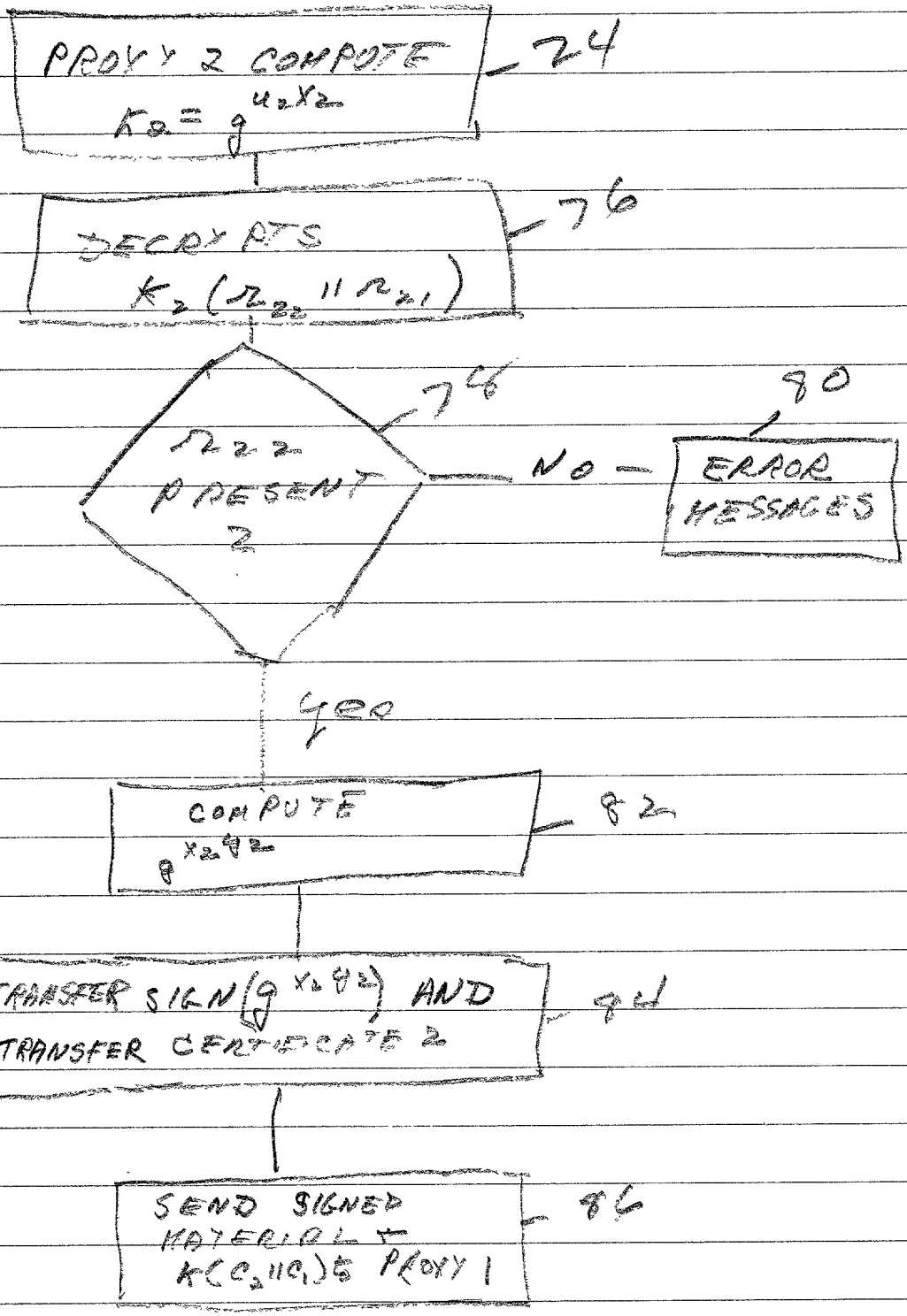
PROXY 2 COMPUTE
$K_2 = g^{u_2 x_2}$
74
DECRYPTS
$K_2(r_{22} \| r_{21})$
76
r_{22} PRESENT 2
78
NO
80
ERROR MESSAGES
YES
COMPUTE
$g^{x_2 y_2}$
82
TRANSFER SIGN $(g^{x_2 y_2})$ AND TRANSFER CERTIFICATE 2
84
SEND SIGNED MATERIAL + $K(C_2 \| r_1)$ TO PROXY 1
86

FIG 6

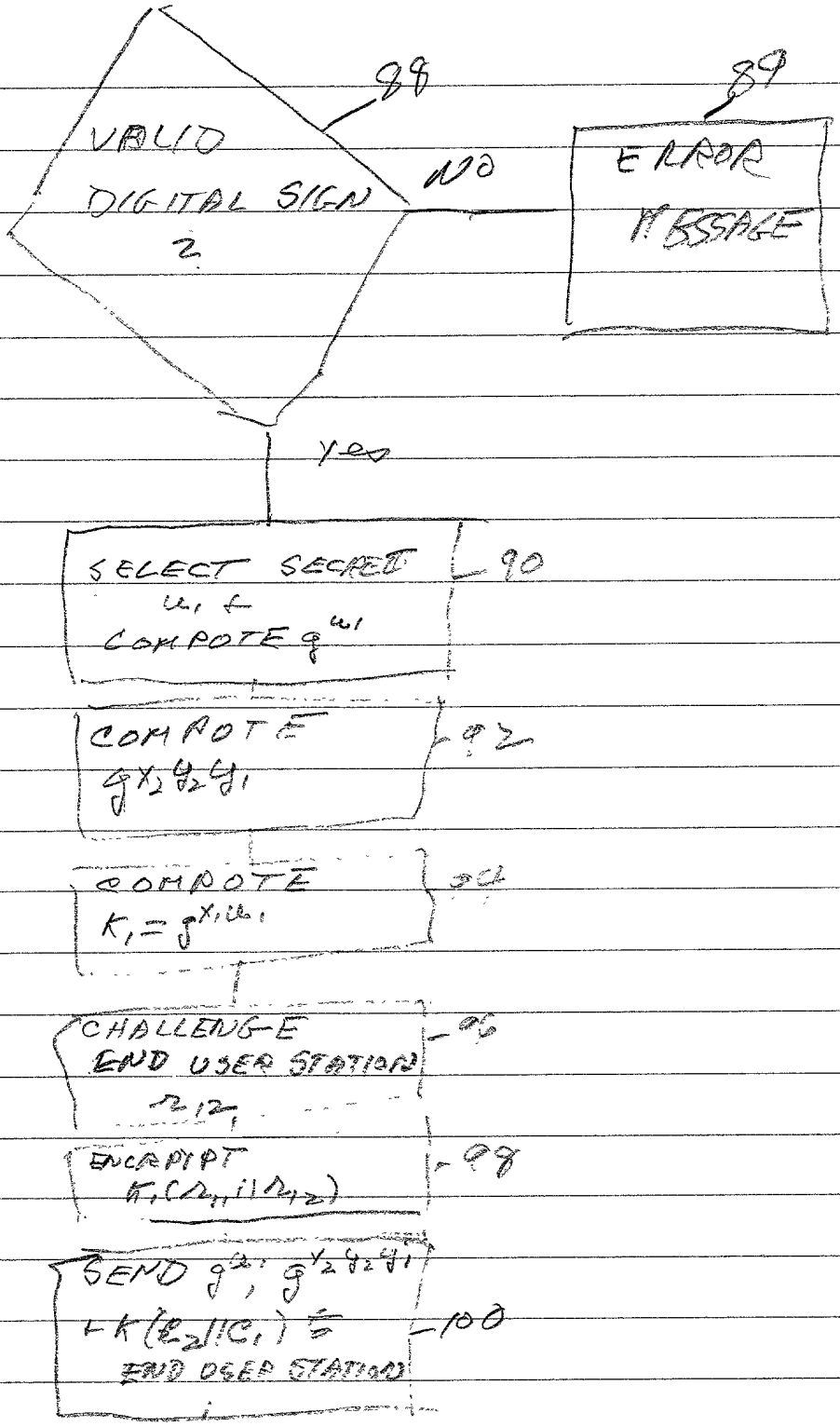
98
VALID DIGITAL SIGN 2.
NO
99
ERROR MESSAGE
YES
SELECT SECRET u_1 & COMPUTE g^{u_1}
90
COMPUTE $g^{x_2 y_2 y_1}$
92
COMPUTE $K_1 = g^{x_1 u_1}$
94
CHALLENGE END USER STATION 2 r_1
96
ENCRYPT $K_1(r_1 || r_2)$
98
SEND g^{x_1}, $g^{x_2 y_2 y_1}$ $+K(E_2 || C_1)$ END USER STATION 1
100

FIG 7

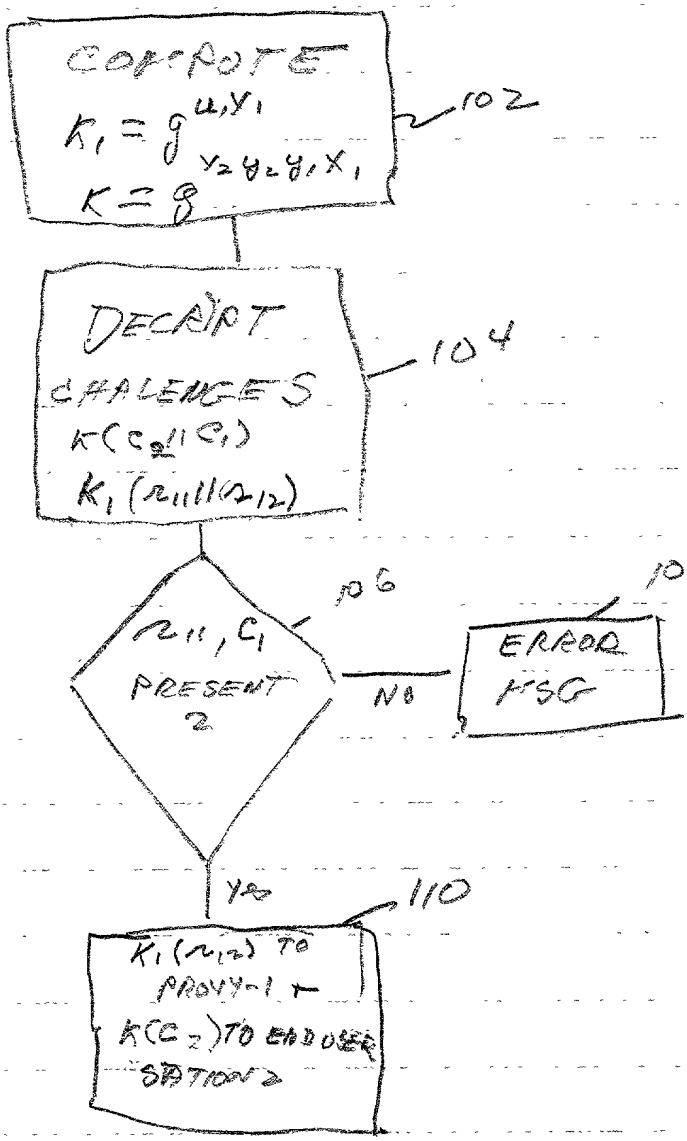
COMPUTE
$K_1 = g^{u,y_1}$
$y_2 y_3 y_4 x_1$
$K = g$
102
DECRYPT
CHALLENGES
$K(C_2 || C_1)$
$K_1(r_{11} || r_{12})$
104
r_{11}, C_1
PRESENT
2
106
NO
ERROR
MSG
108
YES
110
$K_1(r_{12})$ TO
PROXY-1
$K(C_2)$ TO END USER
STATION 2

FIG 8

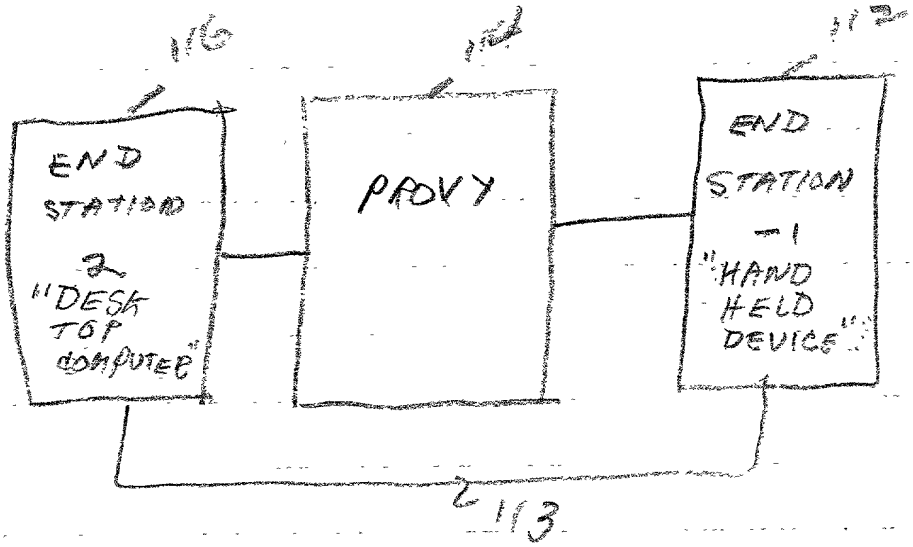

Fig 9

Docket No. 50325-0103

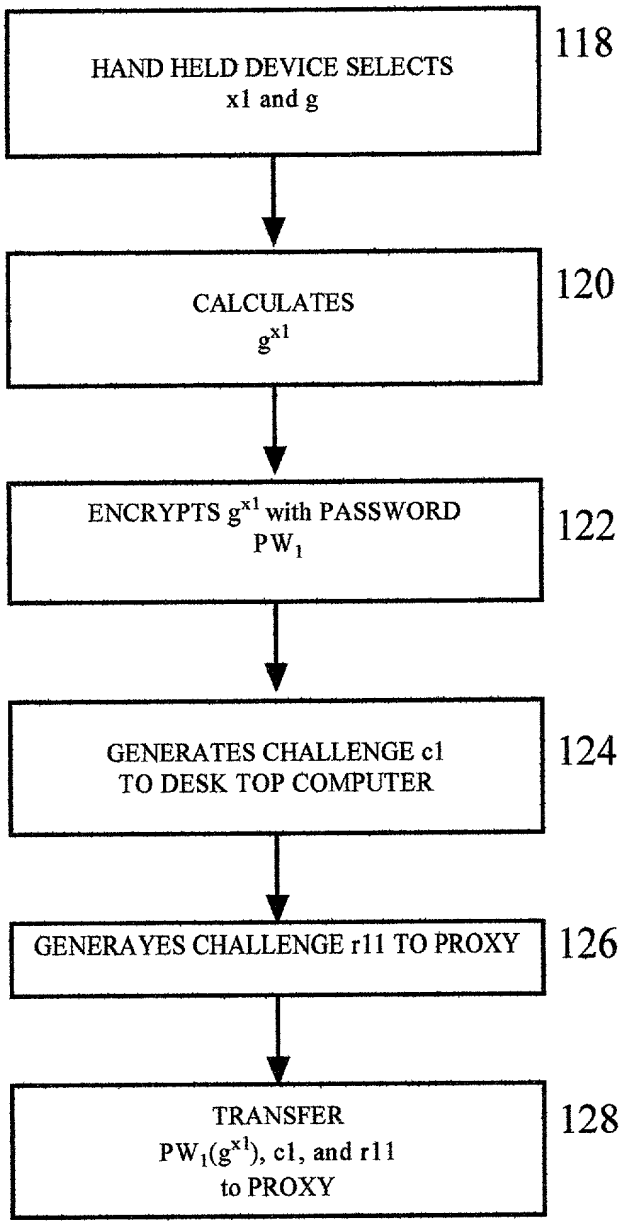
HAND HELD DEVICE SELECTS
x1 and g
118
CALCULATES
g^{x1}
120
ENCRYPTS g^{x1} with PASSWORD
PW_1
122
GENERATES CHALLENGE c1
TO DESK TOP COMPUTER
124
GENERAYES CHALLENGE r11 TO PROXY
126
TRANSFER
$PW_1(g^{x1})$, c1, and r11
to PROXY
128

FIG 10

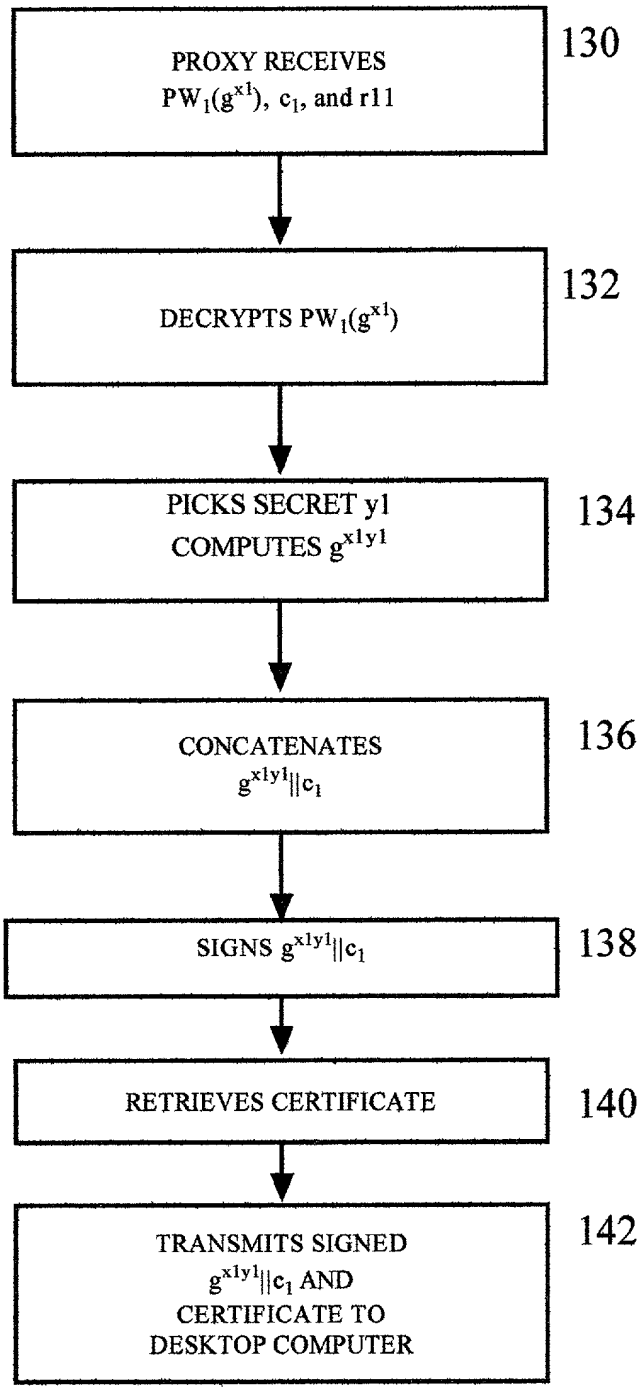
PROXY RECEIVES
$PW_1(g^{x1})$, c_1, and r11
130
DECRYPTS $PW_1(g^{x1})$
132
PICKS SECRET y1
COMPUTES g^{x1y1}
134
CONCATENATES
$g^{x1y1}||c_1$
136
SIGNS $g^{x1y1}||c_1$
138
RETRIEVES CERTIFICATE
140
TRANSMITS SIGNED
$g^{x1y1}||c_1$ AND
CERTIFICATE TO
DESKTOP COMPUTER
142

FIG 11

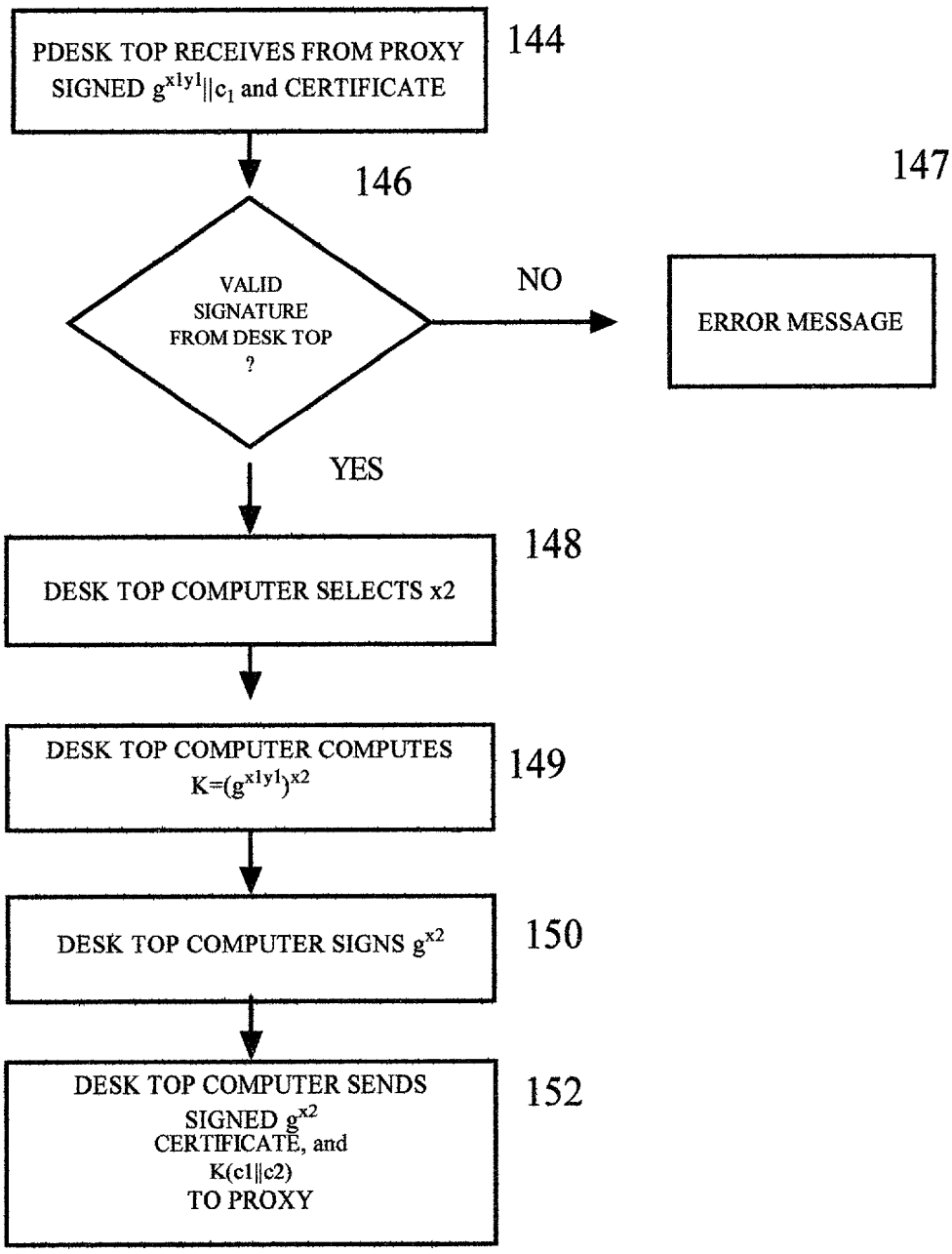
PDESK TOP RECEIVES FROM PROXY SIGNED $g^{x1y1}||c_1$ and CERTIFICATE
144
146
147
VALID SIGNATURE FROM DESK TOP ?
NO
ERROR MESSAGE
YES
DESK TOP COMPUTER SELECTS x2
148
DESK TOP COMPUTER COMPUTES $K=(g^{x1y1})^{x2}$
149
DESK TOP COMPUTER SIGNS g^{x2}
150
DESK TOP COMPUTER SENDS SIGNED g^{x2} CERTIFICATE, and K(c1||c2) TO PROXY
152

FIG 12

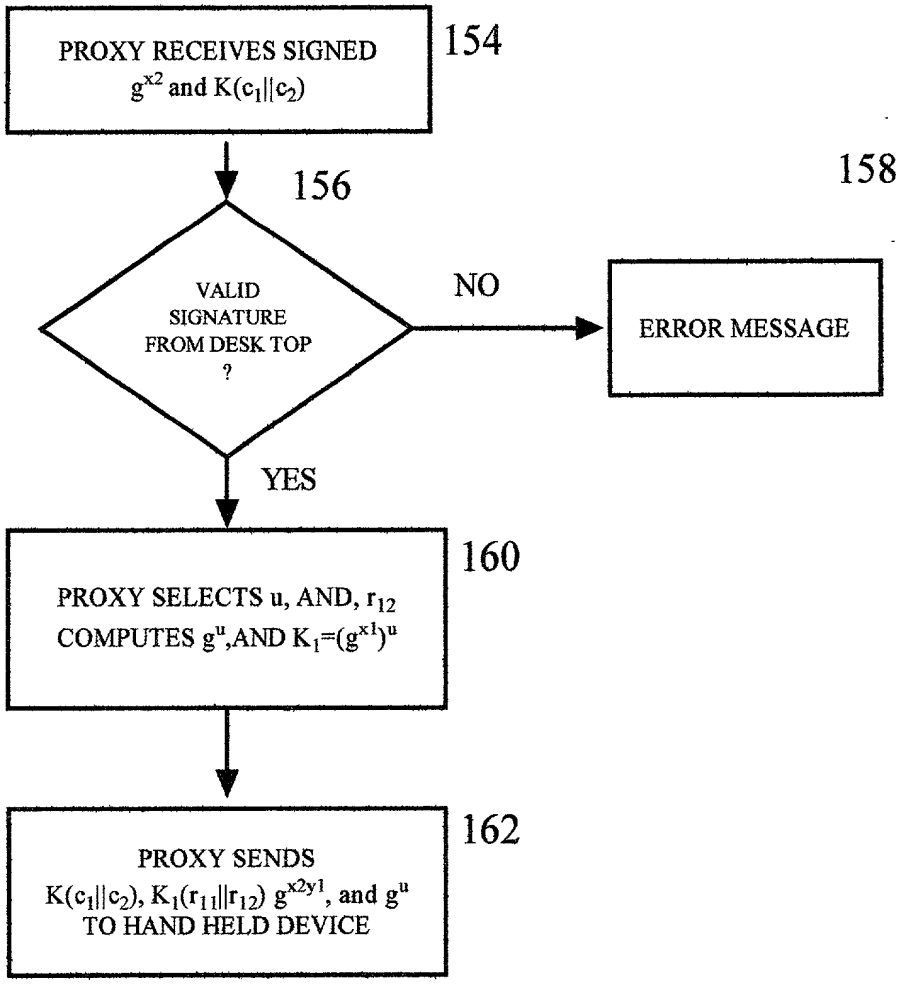
PROXY RECEIVES SIGNED
g^{x2} and $K(c_1||c_2)$
154
156
158
VALID
SIGNATURE
FROM DESK TOP
?
NO
ERROR MESSAGE
YES
PROXY SELECTS u, AND, r_{12}
COMPUTES g^u,AND $K_1=(g^{x1})^u$
160
PROXY SENDS
$K(c_1||c_2)$, $K_1(r_{11}||r_{12})$ g^{x2y1}, and g^u
TO HAND HELD DEVICE
162

FIG 13

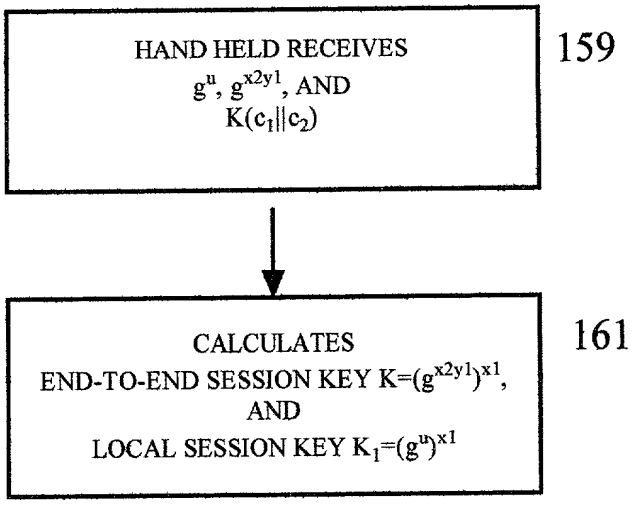
HAND HELD RECEIVES
g^u, g^{x2y1}, AND
$K(c_1||c_2)$
159
CALCULATES
END-TO-END SESSION KEY $K=(g^{x2y1})^{x1}$,
AND
LOCAL SESSION KEY $K_1=(g^u)^{x1}$
161

FIG 14

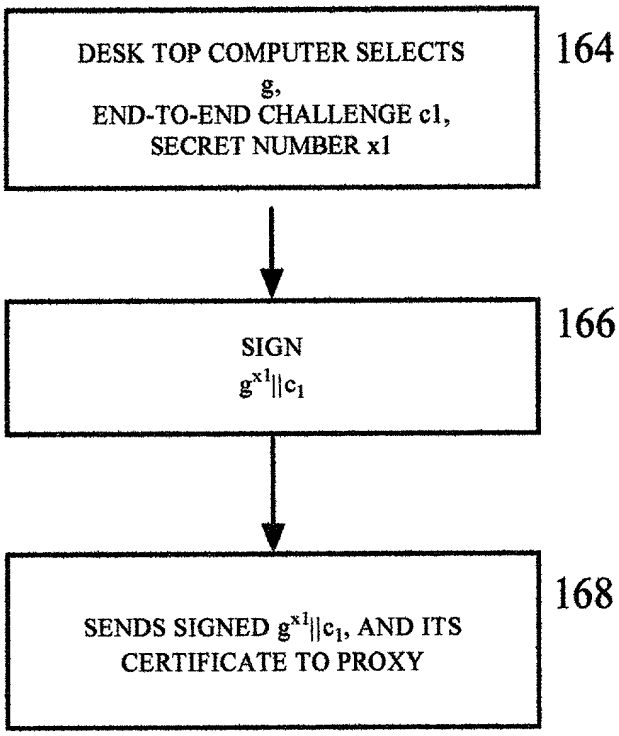
DESK TOP COMPUTER SELECTS
g,
END-TO-END CHALLENGE c1,
SECRET NUMBER x1
164
SIGN
$g^{x1}||c_1$
166
SENDS SIGNED $g^{x1}||c_1$, AND ITS
CERTIFICATE TO PROXY
168

FIG 15

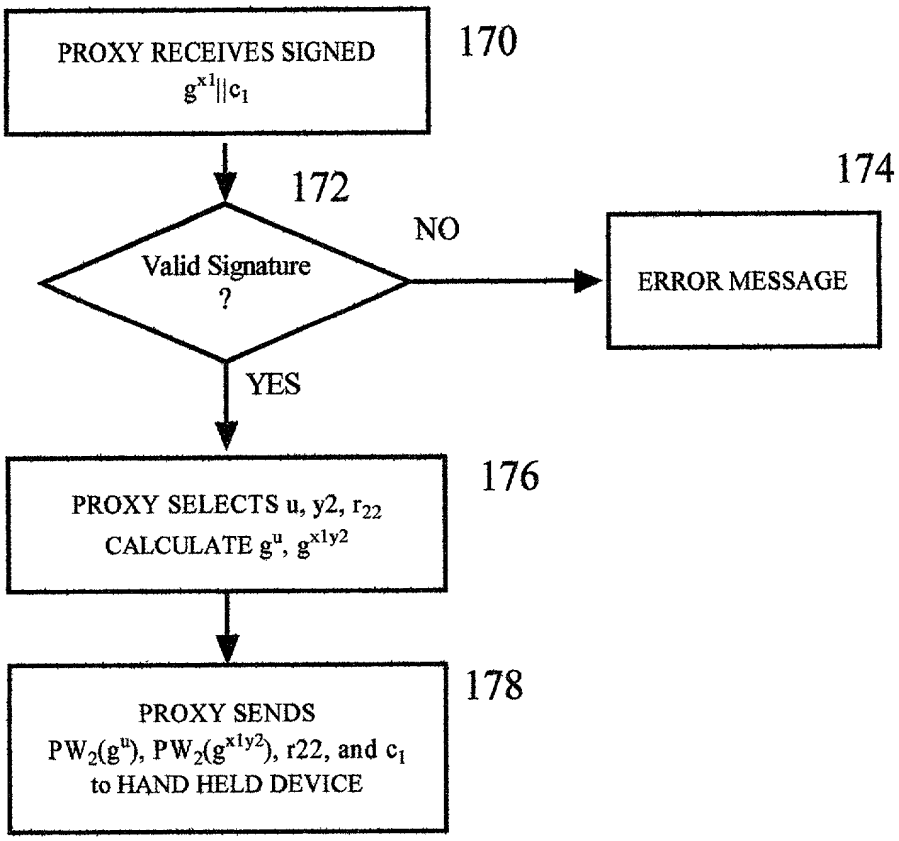
PROXY RECEIVES SIGNED
$g^{x1}||c_1$
170
172
Valid Signature
?
NO
174
ERROR MESSAGE
YES
PROXY SELECTS u, y2, r_{22}
CALCULATE g^u, g^{x1y2}
176
PROXY SENDS
$PW_2(g^u)$, $PW_2(g^{x1y2})$, r22, and c_1
to HAND HELD DEVICE
178

FIG 16

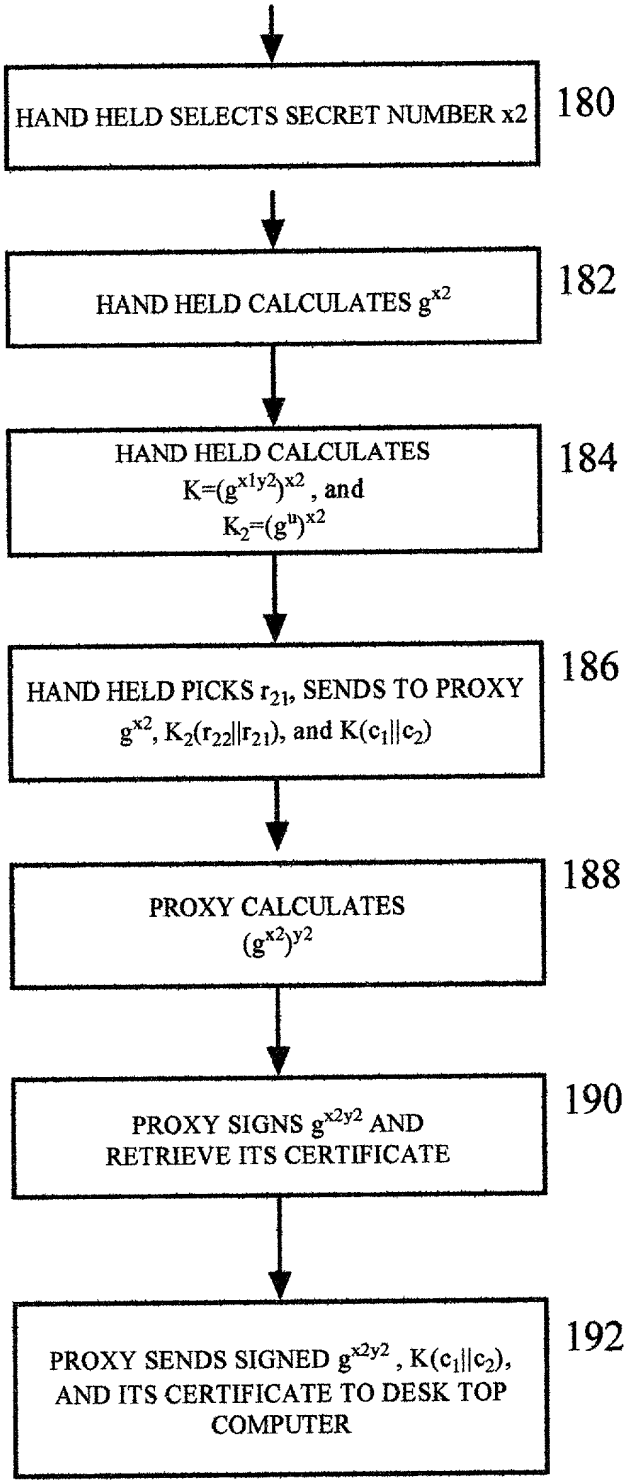
HAND HELD SELECTS SECRET NUMBER x2
180
HAND HELD CALCULATES g^{x2}
182
HAND HELD CALCULATES
$K=(g^{x1y2})^{x2}$, and
$K_2=(g^{y})^{x2}$
184
HAND HELD PICKS r_{21}, SENDS TO PROXY
g^{x2}, $K_2(r_{22}||r_{21})$, and $K(c_1||c_2)$
186
PROXY CALCULATES
$(g^{x2})^{y2}$
188
PROXY SIGNS g^{x2y2} AND
RETRIEVE ITS CERTIFICATE
190
PROXY SENDS SIGNED g^{x2y2}, $K(c_1||c_2)$,
AND ITS CERTIFICATE TO DESK TOP
COMPUTER
192

FIG 17

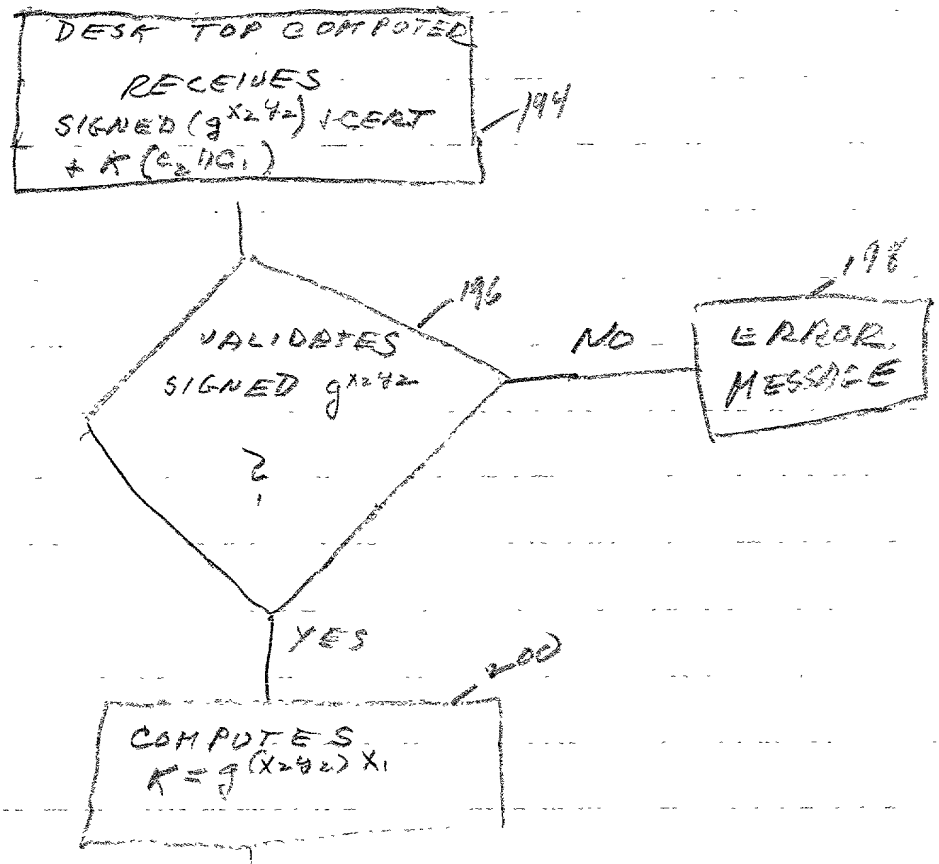
DESK TOP COMPUTER
RECEIVES
SIGNED ($g^{X_2 Y_2}$) VCERT
+ T (E_2, ID$_1$)
194
VALIDATES
SIGNED $g^{X_2 Y_2}$
?
196
NO
ERROR MESSAGE
198
YES
COMPUTES
$K = g^{(X_2 Y_2) X_1}$
200

FIG 18